HP0-A116 Q&As

HP ArcSight ESM 6.5 Security Administrator and Analyst

Pass HP HP0-A116 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/hp0-a116.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which ArcSight ESM user type provides full privileges to use the Command Center, the ArcSight Console, the Arcsight Web client, and all tools?

A. Web User

B. Normal User

C. Connector Installer

D. Management Tool

Correct Answer: B

QUESTION 2

Which processes occur in the first phase of the event lifecycle? (Select two.)

A. evaluating event data

B. applying event categories

C. applying hashing to event data

D. correlating event data

E. normalizing event data

Correct Answer: BE

QUESTION 3

Using SSL technology, information can be communicated over an encrypted channel. What is SSL?

A. Secure Sockets Layer

B. Security Standards Layer

C. Smart Stealth Layer

D. Standard Security Layer

Correct Answer: A

QUESTION 4

Which command is a valid investigate command?

A. Add [Attribute=Value] to Filter

B. Create [Filter=Value]

C. Add [Value!=Condition] to Filter

D. Add to Filter [List of Related Conditions]

Correct Answer: A

QUESTION 5

What is a function of the Variable GetSessionData?

A. retrieves data fields from a Session List

B. sends session details to the ArcSight Manager

C. populates a Session List

D. investigates session details in the audit log

Correct Answer: A

QUESTION 6

Which role does the Active Channel play in testing a rule?

A. The rule can be replayed and verified against real-time events in the Active Channel.

B. The rule can be replayed against historical events in the Active Channel.

C. The rule cannot be tested with the Active Channel because it will create additional invalid Correlation events.

D. The rule can only be tested with an Active Channel by an administrator.

Correct Answer: B

QUESTION 7

What are potential ways of acknowledging notifications? (Select two.)

A. by replying to notification email

B. by calling in to the notification response hotline

C. by sending email to SysAdmin

D. by using the Notifications Manager in the ArcSight Console

Correct Answer: AD

QUESTION 8

Which statement is true about ArcSight SmartConnectors acting in "passive" mode?

A. They receive events forwarded from originating devices.

B. They pull events from originating devices.

C. They do not process events from devices.

D. They process events for performance testing but then discard them.

Correct Answer: A

QUESTION 9

Why would you lock a Case?

A. to close and archive a Case

B. to prevent others from modifying the Case while you edit or attach something to the Case

C. to prevent the Case from being seen in the Resource List

D. to preserve the state of the Case

Correct Answer: B

QUESTION 10

What are valid actions for a rule to take? (Select two.)

A. send notification

B. execute command

C. generate report

D. add to filter

Correct Answer: AB

QUESTION 11

How do asset categorization and event categorization relate to each other?

A. Asset categorization requires custom FlexConnectors; event categorization uses standard Smartconnectors.

B. Asset categorization and event categorization are the same.

C. Asset categorization is the fingerprint of an asset; event categorization is a set of criteria that describes an event.

D. Asset categorization and event categorization use the same field set to apply categories to assets and events

Correct Answer: D

QUESTION 12

There are three types of ArcSight SmartConnectors. Which type is used primarily to execute commands on a device to retrieve, modify, or analyze its configuration?

A. Event Connectors

B. Scanner Connectors

C. CounterACT Connectors

D. SNMP Connectors

Correct Answer: C

QUESTION 13

Which functions does a non-event based Data Monitor perform?

A. evaluates the event stream and creates Correlation events when anomalies are discovered

B. monitors and displays rule and filter data flow thresholds and latencies

C. summarizes and displays event-based Data Monitor statistics

D. monitors and displays ArcSight ESM system and platform status

Correct Answer: D

QUESTION 14

What is a criteria factor within the ArcSight Priority Formula?

A. Assurance

B. Asset Priority

C. Seriousness

D. Model Confidence

Correct Answer: D

QUESTION 15

When exporting search results, what does the "Save to ArcSight Command Center" option do?

A. automatically exports the file to the Administration > Saved Searches > Saved Search Files path

B. opens a dialog allowing the user to specify a download location on the browser host system

C. opens the appropriate output format application to view and optionally save the results on the user\\'s host

D. automatically exports the file to the ESM host /logger/userdata/savedsearch directory

Correct Answer: A